Культенко Олександр Володимирович
старший викладач кафедри правознавства факультету історії та права Кіровоградського державного педагогічного університету імені Володимира Винниченка, кандидат юридичних наук

АНАЛІЗ САНКЦІЙ КРИМІНАЛЬНИХ КОДЕКСІВ ФРАНЦІЇ, НІМЕЧЧИНИ І ЛЮКСЕМБУРГУ НА ПРОТИДІЮ ЗЛОЧИНАМ У КІБЕРПРОСТОРІ

З розвитком телекомунікації корелюється економічне зростання. Величезна незбалансованість (диспропорції) у доступі до послуг телекомунікаційних систем між промислово розвиненими країнами і тими, які розвиваються, спонукає усе більшу кількість держав вживати заходів спрямованих на урегулювання суспільних відносини у кіберпросторі. Оскільки кіберзлочинність і тероризм становлять серйозну загрозу для суверенітету, інфраструктури, комерційних інтересів, і державної політики, високо розвинені держави з поширенням технологій передавання даних (інформації) перш за все поліпшують свої кримінальні кодекси.

Дослідження які провели у 1999 р. Дрю С. Арена (Drew C. Arena), Сюзен В. Бреннер (Susan W. Brenner), Джордж СС. Чен (George C. C. Chen), Катерина А. Дроздова (Ekaterina A. Drozdova), Марк Д. Гудман (Marc D. Goodman), і Дітріх Нейман (Dietrich Neumann), спрямовані на вивчення кодексів п'ятдесяти країн, пов'язаних з встановленням санкцій на протидію злочинам з застосуванням комп'ютера. Дослідники з'ясували, що 30 % обстежених держав не мало як статей у кодексах, так і спеціальних законів у цій сфері [1, с. 3]

У теперішній час однією зі сфер, в якій національне законодавство держав Європи потребує урегулювання, є комп'ютерний саботаж, який включає в себе цілеспрямоване пошкодження цілісності комп'ютерів, комп'ютерних мереж і комп'ютерних даних. Санкції за зміну ступеня захисту, що надаються комп'ютерам, які зберігають дані, у кримінальних законах європейських держав мають

різні вимоги до намірів і ступеня пошкодження, покликані урегульовувати в основному наслідки вандалізму або хуліганських дій в цілому [2].

Слід вказати на держави, які використовують єдину технологію передачі даних (CSD): Австрія Данія, Німеччина, Фінляндія, Франція, Люксембург, Нідерланди, Іспанія, Швеція та Великобританія [3, с.29].

Зосередимо увагу на чинних санкціях у формі позбавлення волі (далі п.в.) або грошового штрафу в наступних державах (див. табл.1)

Таблиця 1

Санкції кримінальних кодексів Франції, Німеччини і Люксембургу на протидію злочинам у кіберпросторі

Санкції за:	Держава		
	Франція	Німеччина	Люксембург
Неправомірний доступ до інформації	П.в. до 1 року або п.в. до 5 років (якщо суб'єкт є посадовою особою) або грошовий штраф	П.в. до 3 років або грошовий штраф	П.в. від одного місяця до року або грошовий штраф
Неправомірне перехоплення інформації	П.в. до 1 року або п.в. до 5 років (якщо суб'єкт є посадовою особою) або грошовий штраф	П.в. до 3 років або грошовий штраф	П.в. від одного місяця до року або грошовий штраф
Неправомірна модифікація інформації	П.в. до 3 років або грошовий штраф	П.в. до 5 років або грошовий штраф	П.в. до 2 років або грошовий штраф
Неправомірний доступ до систем зв'язку	П.в. до 2 років або грошовий штраф	П.в. до 3 років або грошовий штраф	П.в. від 3 місяців до 3 років або грошовий штраф
Незаконний збір комп'ютерної інформації	П.в. до 1 року або п.в. до 5 років (якщо суб'єкт є посадовою особою) або грошовий штраф	П.в. до 3 років або грошовий штраф	П.в. від одного місяця до року або грошовий штраф
Створення шкідливих програм	П.в. до 3 років або грошовий штраф	П.в. до 5 років або грошовий штраф	П.в. від 3 місяців до 3 років або грошовий штраф
DoS-атака	П.в. до 3 років або грошовий штраф	П.в. до 5 років або грошовий штраф	П.в. від 3 місяців до 3 років або грошовий штраф
Спроба вторгнення	П.в. до 2 років або грошовий штраф	П.в. до 3 років або грошовий штраф	П.в. від 2 місяців до року або грошовий штраф

А отже, в Україні теж можна застосувати подібні межі покарання для врегулювання такого специфічного виду суспільних відносин.

Додамо, навіть в Європі у своєму законодавстві більш детально розтлумачила терміни у диспозиціях до санкцій на протидію комп'ютерному саботажу і знищенню даних лише невелика кількість держав – Італія, Швеція, Нідерланди. Останні ввели у свої кримінальні кодекси поняття про поширення деструктивних програм таких як віруси, за формою «черв'як» чи «троянський кінь» [4, с. 46]. Для подальшого наукового обґрунтування законопроекту «Про основні засади забезпечення кібербезпеки України» вкажемо на необхідність таких подальших розвідок і в Україні.

Використані джерела:

1. Tonya L. Putnam, David D. Elliott / International Responses to Cyber Crime. Chapter 2 – Hoover Institution Press Stanford University Stanford California, 2000. – 35 p.

2. Laviero Buono / Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3) – New Journal of European Criminal law, Belgium, 2012. – P. 332–344.

3. *Dr. Ulrich Siebe / Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study – University of Wurzburg, Germany, 1998 – 240 p.*

4. *Seymour E. Goodman, Abraham D. Sofae / The Transnational Dimension of Cyber Crime and Terrorism – Hoover Institution Press Stanford University Stanford California, 2001. – 292 p.*